Décomposition de Bruhat

Soient k un corps, $n \geqslant 1$ un entier, et $\mathrm{GL}_n(k)$ le groupe linéaire. Le théorème de décomposition dont il est question s'énonce ainsi : pour toute matrice carrée $A \in \mathrm{GL}_n(k)$, il existe une permutation σ, une matrice unipotente supérieure U et une matrice triangulaire supérieure T telles que $A = UM_\sigma T$ (où M_σ est la matrice de permutation associée à σ), et de plus la permutation σ est unique. Rappelons qu'une matrice unipotente supérieure est une matrice triangulaire supérieure dont les coefficients diagonaux sont tous égaux à 1.

Nous allons établir ce résultat comme conséquence d'un énoncé plus géométrique d'algèbre linéaire. Notons E un espace vectoriel de dimension n sur k. On appelle *drapeau (complet)* de E une suite strictement croissante de sous-espaces vectoriels $F_0 \subsetneq \cdots \subsetneq F_n$. On notera simplement F un tel drapeau ; observez que $\dim(F_i) = i$ pour tout i.

Théorème. *Soient F et G deux drapeaux complets de E. Alors il existe une permutation $\sigma \in \mathfrak{S}_n$ et une base ordonnée $(e_1, \dots, e_n)$ de E telles que $e_i \in F_i \cap G_{\sigma(i)}$ pour tout $i \in \{1, \dots, n\}$. De plus, la permutation $\sigma_{F,G} := \sigma$ est unique.*

Commentaires. (1) Cet énoncé signifie simplement qu'il existe une base de E dont chaque vecteur appartient à l'un des F_i et à l'un des G_j.

(2) L'unicité de $\sigma = \sigma_{F,G}$ implique que $\sigma_{G,F} = {\sigma_{F,G}}^{-1}$, car si l'on pose $\tau = \sigma^{-1}$ et $e'_j = e_{\tau(j)}$ on a $e'_j \in G_j \cap F_{\tau(j)}$ d'où $\tau = \sigma_{G,F}$. Cependant, la preuve procèdera différemment, en montrant *d'abord* que $\sigma_{G,F} = {\sigma_{F,G}}^{-1}$ *puis* que $\sigma_{F,G}$ est unique.

Preuve. Fixons un entier $i \geqslant 1$. On observe que si pour un certain $j = j_0 \geqslant 1$ l'inclusion $F_{i-1} + G_j \subset F_i + G_j$ est une égalité, alors elle l'est encore pour tout $j \geqslant j_0$ puisque $F_{i-1} + G_j = F_{i-1} + G_{j_0} + G_j = F_i + G_{j_0} + G_j = F_i + G_j$. Il s'ensuit que lorsque j croît de 0 à n, cette inclusion qui est stricte pour $j = 0$ devient une égalité pour un certain $j \geqslant 1$, puis le reste. Notons $\sigma_{F,G}(i) = j$ cet entier minimal, qui est donc caractérisé par les relations $F_{i-1} + G_{j-1} \subsetneq F_i + G_{j-1}$ et $F_{i-1} + G_j = F_i + G_j$.

Pour montrer que $\sigma_{F,G}$ est une permutation, il suffit de montrer que $\sigma_{G,F} \circ \sigma_{F,G} = \mathrm{id}$. Pour cela, notons $j = \sigma_{F,G}(i)$ et montrons qu'alors $i = \sigma_{G,F}(j)$, c'est-à-dire $F_{i-1} + G_{j-1} \subsetneq F_{i-1} + G_j$ et $F_i + G_{j-1} = F_i + G_j$. Or supposant que $F_{i-1} + G_{j-1} = F_{i-1} + G_j$, on déduit $F_i + G_{j-1} = F_i + G_j = F_{i-1} + G_j = F_{i-1} + G_{j-1}$ ce qui est une contradiction ; ceci établit l'inclusion stricte désirée. Par ailleurs, on a :

$$\dim(F_i + G_{j-1}) = \dim(F_{i-1} + G_{j-1}) + 1 = \dim(F_{i-1} + G_j) = \dim(F_i + G_j),$$

ce qui montre que l'inclusion $F_i + G_{j-1} \subset F_i + G_j$ est une égalité.

Pour i et j quelconques, utilisant la formule reliant la somme de deux sous-espaces à leur intersection, on voit que $F_{i-1} + G_j = F_i + G_j$ équivaut à $\dim(F_i \cap G_j) = \dim(F_{i-1} \cap G_j) + 1$. Si $j = \sigma(i)$ avec $\sigma = \sigma_{F,G}$, cette égalité a lieu donc on peut choisir $e_i \in F_i \cap G_{\sigma(i)} \setminus F_{i-1} \cap G_{\sigma(i)}$. En particulier, on a $e_i \in F_i \setminus F_{i-1}$ ce qui montre que $(e_1, \dots, e_n)$ est une base (ordonnée) de E.

Montrons enfin que $\sigma_{F,G}$ est unique. Supposons qu'il existe une permutation $\varphi \in \mathfrak{S}_n$ et des vecteurs $e_i \in F_i \cap G_{\varphi(i)}$ formant une base de E. Alors $F_i = \mathrm{Vect}(e_1, \dots, e_i)$ donc $e_i \notin F_{i-1}$. Posant $j = \varphi(i)$, on a donc $\dim(F_i \cap G_j) = \dim(F_{i-1} \cap G_j) + 1$ puis $F_{i-1} + G_j = F_i + G_j$ d'après l'argument sur la somme et l'intersection utilisé quelques lignes plus haut. Il s'ensuit que $\varphi(i)$ est inférieur ou égal à $\sigma_{F,G}(i)$ tel que celui-ci a été défini en début de preuve. Comme ceci vaut pour tout i et que $\sigma_{F,G}$ est une bijection, ceci implique que $\varphi = \sigma_{F,G}$. $\square$

Corollaire 1. *Soit X l'ensemble des paires de drapeaux de E, muni de l'action naturelle de $G = \mathrm{GL}(E)$ définie par $u.(F,G) = (u(F), u(G))$. Alors l'application $(F,G) \mapsto \sigma_{F,G}$ passe au quotient en une bijection canonique entre l'ensemble d'orbites X/G et le groupe symétrique $\mathfrak{S}_n$.*

Cet énoncé dit qu'après transport par un automorphisme de E, le drapeau G est obtenu par (unique) permutation des vecteurs d'une base de F. Autrement dit, à automorphisme linéaire et à permutation près, il n'y a qu'un drapeau dans E. Si $E = k^n$, on peut choisir par exemple le drapeau canonique F tel que F_i est engendré par les i premiers vecteurs de la base canonique.

Preuve. Soient $\sigma = \sigma_{F,G}$ et (e_i) une base satisfaisant les conclusions du théorème. On a alors $G_j = \mathrm{Vect}(e_{\sigma^{-1}(1)}, \ldots, e_{\sigma^{-1}(j)})$ puisque pour chaque $k \leqslant j$ le vecteur $e_{\sigma^{-1}(k)}$ appartient à G_k qui est inclus dans G_j, et ces vecteurs sont en nombre $j = \dim(G_j)$. Ainsi G est entièrement déterminé par la base ordonnée (e_i) et la permutation σ. Si l'on fixe une base ordonnée $\mathscr{B}$ de E et qu'on note $u \in \mathrm{GL}(E)$ l'unique automorphisme linéaire qui envoie (e_i) sur $\mathscr{B}$, on voit que la paire $(u(F), u(G))$ est entièrement déterminée par σ. Notez qu'on a utilisé la base $\mathscr{B}$ non pas pour définir l'application $X/G \to \mathfrak{S}_n$, qui est donc bien canonique, mais seulement pour vérifier que c'est une bijection. $\square$

Revenons aux notations de départ pour en déduire la décomposition de Bruhat sous sa forme matricielle. On observera que la preuve du corollaire 2 utilise seulement le théorème, pas le corollaire 1. On rappelle que M_σ désigne la matrice de permutation associée à σ.

Corollaire 2. *Pour tout $A \in \mathrm{GL}_n(k)$, il existe une permutation σ, une matrice U unipotente supérieure et une matrice T triangulaire supérieure, telles que $A = UM_\sigma T$. De plus σ est unique.*

Preuve. Notons $f = (f_1, \ldots, f_n)$ la base (ordonnée) canonique de $E = k^n$ et $g = (g_1, \ldots, g_n)$ la base (ordonnée) formée par les vecteurs colonnes de la matrice A. Ainsi A n'est autre que la matrice de l'identité exprimée dans les bases g à la source et f au but, c'est-à-dire, en symboles $A = \mathrm{Mat}_{g,f}(\mathrm{id})$.

Soient F, G les deux drapeaux de E définis par $F_i = \mathrm{Vect}(f_1, \ldots, f_i)$ et $G_j = \mathrm{Vect}(g_1, \ldots, g_j)$. Notons $\sigma = \sigma_{F,G}$ et $e = (e_1, \ldots, e_n)$ la base ordonnée fournie par le théorème, qui vérifie $e_i \in F_i \cap G_{\sigma(i)}$. Puisque $e_i \in F_i \setminus F_{i-1}$, lorsqu'on exprime e_i sur la base f sa composante sur f_i est non nulle ; quitte à normaliser e_i on peut donc supposer que cette composante est 1. Ceci signifie que la matrice de passage $U = \mathrm{Mat}_{e,f}(\mathrm{id})$ est unipotente supérieure.

Notons maintenant $\tau = \sigma^{-1}$ et $e'_i = e_{\tau(i)}$; clairement la matrice de passage $\mathrm{Mat}_{e',e}(\mathrm{id})$ est la matrice de permutation M_σ. Les vecteurs e'_i vérifient $e'_i \in F_{\tau(i)} \cap G_i$ et le raisonnement fait précédemment montre que la matrice de passage $T = \mathrm{Mat}_{g,e'}(\mathrm{id})$ est triangulaire supérieure (mais on ne peut plus normaliser de manière à ce qu'elle soit unipotente, car cela changerait la normalisation de e_i). On conclut en disant que la matrice de l'application composée

$$\begin{tikzcd}
(E,g) \arrow[r, "\mathrm{id}"] \arrow[r, bend right, dotted, "T"'] \arrow[rrr, bend left, dashed, "A"] & (E,e') \arrow[r, "\mathrm{id}"] \arrow[r, bend right, dotted, "M_\sigma"'] & (E,e) \arrow[r, "\mathrm{id}"] \arrow[r, bend right, dotted, "U"'] & (E,f)
\end{tikzcd} ,$$

écrite dans les bases indiquées, est le produit de matrices $A = UM_\sigma T$. $\square$